UNITED STATES PATENT APPLICATION

for

TECHNIQUE TO ESTABLISH WIRELESS SESSION KEYS SUITABLE FOR ROAMING

Inventor:
Jesse R. Walker

File No: 42390.P9007

Prepared by:
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026
(408) 720-8598

TECHNIQUE TO ESTABLISH WIRELESS SESSION KEYS SUITABLE FOR ROAMING

FIELD OF THE INVENTION

This invention relates to authentication technologies generally and particularly to authentication techniques in a wireless network.

BACKGROUND OF THE INVENTION

A wireless network is a flexible data communication medium implemented as an extension for, or as an alternative to, a wired network. By using radio frequency (RF) technology, wireless networks transmit and receive data over air, minimizing the need and the cost typically associated with wired connections. Moreover, wireless networks offer mobility and flexibility for users. For example, doctors and nurses in hospitals are able to use hand-held devices or notebook computers to access patient information from a server through wireless networks without having to search for a physical jack to plug their devices or computers into.

Figure 1 demonstrates a prior art wireless network configuration. Specifically, the network configuration comprises wireless stations 108 and 110, wireless medium 106 and access points 100, 102 and 104. Wireless stations 108 and 110 communicate with access points 100, 102 and 104 through electromagnetic airwaves 106. Access points 100, 102 and 104 are also connected to wired network 112 and have access to the network resources of wired network 112 such as, server

114, network printer 116 or other devices coupled to wired network 112. It should be noted that wireless stations 108 and 110 are not stationary and do not have to communicate with particular multiple access points. For instance, wireless station 108 may seamlessly move from the coverage area of access point 100 to the coverage area of access point 104 and still maintain its data connections with the access points.

Despite the portability and the convenience that wireless technology offers, there still lacks a comprehensive security scheme to ensure privacy and integrity of the data on wireless networks. For instance, one existing approach is to utilize static keys to encrypt data on a wireless link. Such encrypted data are vulnerable to attack, because the probability of deciphering them is much greater than if the data were encrypted with constantly changing keys. Another approach involves a wireless station sharing a group key with an access point. Thus, when any one device on a wireless network falls into the hands of an attacker, the security of every system in the network is compromised. Yet another approach has every wireless station share one key. As a result, any wireless station is capable of decrypting the traffic of any other wireless.

As has been demonstrated, an improved method and an apparatus are needed to enhance the security of a wireless network.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and is not limited by the figures of the accompanying drawings, in which like references indicate similar elements, and in which:

Figure 1 illustrates a prior art wireless network configuration.

Figure 2 illustrates one embodiment of the present invention, a secured wireless roaming system.

Figure 3(a) illustrates a block diagram of one embodiment of a wireless station in accordance with the present invention.

Figure 3(b) illustrates a block diagram of one embodiment of an access point in accordance with the present invention.

Figure 4 illustrates a flow chart of one process that one embodiment of a wireless station in accordance with the present invention follows.

Figure 5 illustrates a flow chart of one process that one embodiment of an access point in accordance with the present invention follows.

DETAILED DESCRIPTION

A method and an apparatus for establishing secured roaming are disclosed. In the following description, numerous specific details are set forth, such as Kerberos protocol, etc. in order to provide a thorough understanding of the present invention. However, it will be apparent to one of ordinary skill in the art that the invention may be practiced without these particular details. In other instances, well-known elements and theories such as cryptography systems, etc. have not been discussed in special details in order to avoid obscuring the present invention.

In addition, the term, "wireless station", is used throughout the following discussion to refer to any network device that uses some wireless Local Area Network (hereinafter LAN) technology to communicate with a wired network. It can be either an end system or a switching element. Also, a "secured" session refers to information exchanges between two networking devices, where some form of security measures safeguard such exchanges. A "replay attack" describes one form of an attack on a security system. Specifically, a perpetrator who launches such an attack intercepts messages destined for a recipient and replays those intercepted messages back to the recipient.

Unless specifically stated otherwise, the term, "Kerberos protocol", refers to Kerberos Version 5, released on May 5, 1995. It is an authentication protocol that allows entities to authenticate their identities to one another over physically insecure

networks and at the same time still prevents eavesdropping and replay attacks. It also incorporates cryptography systems to further provide for data stream integrity (such as detection of modification) and secrecy (such as preventing authorized reading). The Kerberos protocol operates within the Kerberos infrastructure, which comprises, but not limited to, the following:

1) Key Distribution Center (KDC): maintains and controls the distribution of session keys. A KDC is also considered as a special type of an authentication server in the following discussions.

2) Session key: information that enables two systems to establish a secured session. Session keys have limited life span. Thus, if a secured session is not established within a certain period of time, a new session key is needed.

3) Kerberos client: initiates key distribution from the KDC and then uses the distributed session key to initiate a session with a peer.

4) Kerberos server: the peer system with which the Kerberos client wishes to establish a secured session.

5) Ticket: a Kerberos data structure that grants access of the Kerberos client to the Kerberos server.

6) Authenticator: a Kerberos data structure that Kerberos client uses to authenticate itself to a Kerberos server and also to challenge the Kerberos server to authenticate itself to the Kerberos client.

7) Response: a Kerberos data structure that the Kerberos server uses to authenticate itself to the Kerberos client.

Figure 2 illustrates one embodiment of the present invention or secured wireless roaming system (hereinafter SWRS) 200. SWRS 200 comprises one or more specially configured wireless stations, such as wireless station 202, at least two specially configured access points, such as access points 206 and 208 and authentication server 210. Access points 206 and 208 are coupled to authentication server 210 via wired network 212 and are further coupled to wireless station 202 via wireless network 204. Authentication server 212 is responsible for maintaining and providing security information and safeguarding the integrity of wired network 212 and wireless network 204. The interactions among access points 206 and 208, wireless station 202 and authentication server 212 for creating a secured roaming environment will be discussed with examples in the subsequent section that details the operations of SWRS 200.

Figure 3(a) illustrates a block diagram of one embodiment of wireless station 202. Wireless station 202 comprises control unit 300, transmitter 302, receiver 304, filter 306 and antenna 308. Control unit 300 is mainly responsible for, but not limited to, preparing data for transmission and consuming received data. One embodiment of control unit 300 includes two functional blocks: encryption/decryption engine 314 and authentication protocol engine 316. An

alternative embodiment of control unit 300 may also incorporate a frequency channel selector to dynamically choose an appropriate frequency channel for wireless station 202. Encryption/decryption engine 314 encrypts data that wireless station 202 transmits and decrypts data that wireless station 202 receives with appropriate keys. Additionally, authentication protocol engine 316 contains procedures for wireless station 202 to adhere to in order to further protect the overall integrity of wireless network 204 and wired network 212. Specific examples of the mentioned authentication procedures will be provided in the subsequent section.

Transmitter 302 and receiver 304 share antenna 308. On receive path 310, filter 306 filters out signals received by antenna 308 that are outside of a predetermined frequency range. Receiver 304 is then responsible for extracting data from the filtered signals and passing the resulting data to control unit 300. On transmit path 312, control unit 300 sends prepared data to transmitter 302. Transmitter 302 modulates the prepared data with a carrier of proper frequency and sends the modulated signal to filter 306. Filter 306 again eliminates spurious signal outside of the desired frequency range before transmitting the final filtered signal through antenna 308.

Figure 3(b) demonstrates a block diagram of one embodiment of access point 206 (or access point 208). Similar to wireless station 202, access point 206 also has control unit 318, transmitter 320, receiver 322, filter 324 and antenna 326. Its

control unit 318 has encryption/decryption engine 324 and authentication protocol engine 326 that perform the same functions for access point 206 as encryption/decryption engine 314 and authentication protocol engine 316 do for wireless station 202. In addition, access point 206 has wired-network connection interface 328 to communicate with wired network 212 as shown in Figure 2.

OPERATIONS OF A WIRELESS STATION AND ACCESS POINTS IN A SECURED WIRELESS ROAMING SYSTEM

One specific embodiment of SWRS 200 mainly applies the Kerberos protocol to secure communications among wireless station 202 and access points 206 and 208. In other words, authentication protocol engine 316 (Figure 3(a)) of wireless station 202 and authentication protocol engine 336 (Figure 3(b)) of access points 206 and 208 are specially configured to execute authentication procedures and to handle data structures specified by the Kerberos protocol. However, these mentioned authentication protocol engines 316 and 336 also perform tasks that are either absent or distinct from the Kerberos protocol.

Figure 4 describes a flow chart of one process that one embodiment of wireless station 202 follows. This figure assumes the following: 1) authentication server 210 as shown in Figure 2 is the KDC; 2) wireless station 202 does not yet have the session key to set up a secured session with access point 206, or $session\_key_{206}$; 3) wireless station 202 is currently in the coverage area of access

point 206 and will "roam" in the coverage area of access point 208; 4) access points 206 and 208 share one group identification, ID_g; and 5) the session key for wireless station 202 to establish a secured session with access point 208 is denoted as $session\_key_{208}$.

In conjunction with Figures 2 and 3, instead of acting like a Kerberos client as in a typical application of the Kerberos protocol, authentication protocol engine 316 instructs wireless station 202 to behave as a Kerberos server and provides access point 208 with its identity information in block 400. Then authentication protocol engine 316 waits to respond to access point 206's attempt to establish a secured session using the newly obtained $session\_key_{206}$ in block 402. A session is considered secured when wireless station 202 and access point 206 complete their mutual authentication within the lifetime of $session\_key_{206}$. After authentication protocol engine 316 confirms that a secured session has been established, wireless station 202 obtains ID_g from access point 206. ID_g enables wireless station 202 to access all the access points that share the same ID_g, such as access point 208.

However, wireless station 202 cannot proceed to establish a secured session with access point 208 unless it has another valid session key, or $session\_key_{208}$. As wireless station 202 moves into the coverage area of access point 208, authentication protocol engine 316 switches wireless station 202's role back to being a Kerberos client and requests for $session\_key_{208}$ from authentication server 210. It is important

to note that in a typical application of the Kerberos protocol, a Kerberos client needs to have the identity information of a peer system prior to initiating a session with such a system. In contrast, one embodiment of wireless station 202 simply uses $session\_key_{208}$ and ID_g to initiate a session with access point 208.

Figure 5 illustrates a flow chart of one process that one embodiment of access point 206 (Figure 2) follows. This figure also relies on the same five assumptions described above. In parallel to the discussion for wireless station 202 above, authentication protocol engine 336 instructs access point 206 to behave as a Kerberos client instead of a Kerberos server. Thus, access point 206 initiates session key distribution from authentication server 210 and attempts to establish a secured session with wireless station 202 using $session\_key_{206}$ in block 500. After a secured session has been established in block 502, authentication protocol engine 336 provides wireless station 202 with ID_g in block 504.

Authentication protocol engine 336 then dictates access point 206 to serve as a proxy, or a relay agent, for wireless station 202. As a result, when access point 206 receives a session key request message, such as a ticket request message, from wireless station 202, encryption/decryption engine 334 decrypts the message and authentication protocol engine 336 relays the decrypted message to authentication server 210 in block 506. Similarly, authentication protocol engine 336 also relays $session\_key_{208}$ from authentication server 210 to wireless station 202 after the

session key becomes available. However, before the actual relay occurs, authentication protocol engine 336 appends certain information to $session\_key_{208}$ to set the lifetime of the session key in block 508. In one embodiment, authentication protocol engine 336 selects and appends the current time of day, T, and a random number, N, to the session key.

In addition to the block diagrams as shown in Figures 2, 3(a) and 3(b) and flow charts as shown in Figures 4 and 5, the following tables further demonstrate implementation details of one embodiment of SWRS 200. Phase 1 corresponds to blocks 400, 402 and 404 as illustrated in Figure 4 and blocks 500, 502 and 504 as illustrated in Figure 5. Phase 2 corresponds to blocks 408, 506 and 508. At last, phase 3 corresponds to block 410.

Phase 1:

Actions	Explanations
Wireless station 202 → access point 206: ID_w	Wireless station 202 sends its identity information to access point 206.
Access point 206 → KDC: $ID_{ap\ 206}$, ID_w, $N_{ap\ 206}$	In addition to the identity information of access point 206 and wireless station 202, access point 206 also creates and sends a randomly generated number, $N_{ap\ 206}$, to KDC. This message that access point 206 sends to KDC is also referred to as the *ticket request message*.
KDC → access point 206: $E(K_w; K_{206}, ID_{ap\ 206}, L_{ap\ 206})$, $E(K_{ap}; K_{206}, N_{ap\ 206}, L_{ap\ 206}, ID_w)$ Note 1: The notation, E(K, ***), means that *** is encrypted using encryption key K.	After KDC generates session key, K_{206}, KDC encrypts the session key with encryption keys of wireless station 202, K_w, and of access point 206, K_{ap}, and sends the encrypted messages to access point 206. These messages are also referred to as the *ticket granting message*. Encryption/decryption engine 334 of access

Note 2: Session key, K_{206}, has a lifetime of $L_{ap\ 206}$.	point 206 deciphers part of the ticket granting message using the encryption key, K_{ap}, that it already has knowledge of and passes on the decrypted message to authentication protocol engine 336. Authentication protocol engine 336 proceeds to verify the value of $N_{ap\ 206}$ to ensure that the integrity of the information from KDC has not been compromised.
Access point 206 → wireless station 202: $E(K_w; K_{206}, ID_{ap\ 206}, L_{ap\ 206}), E(K_{206}; ID_{ap\ 206}, T_1)$ Note: T_1 represents the time that access point 206 issues this challenge message.	Authentication protocol engine 336 of access point 206, as has been discussed before, has access point 206 act as a Kerberos client and sends its targeted Kerberos server, wireless station 202, a challenge message. A challenge message includes a ticket and an authenticator. In this case, the ticket is $E(K_w; K_{206}, ID_{ap\ 206}, L_{ap\ 206})$, and the authenticator is $E(K_{206}; ID_{ap\ 206}, T_1)$.

Wireless station 202 → access point 206: $E(K_{206}; T_1)$	Wireless station 202 has from time T_1 to $T_1 + L_{ap\ 206}$ to authenticate itself to access point 206 by sending this response message, $E(K_{206}; T_1)$, to access point 206.
Access point 206 → wireless station 202: $E(K_{206}; ID_g)$	Access point 206 shares the group identity information with wireless station 202.

Phase 2

Actions	Explanations
Wireless station 202 → access point 206: $E(K_{206}; ID_w, ID_g, N_w)$ Note: N_w is a random number that wireless station 202 generates.	As has been mentioned in prior sections, wireless station 202 has changed back to being a Kerberos client. It generates and sends a ticket request message to access point 206 secured by session key, K_{206}.
Access point 206 → KDC: ID_w, ID_g, N_w	Access point 206 serves as a proxy for wireless station 202.
KDC → access point 206: $E(K_g; K_{208}, ID_w, L_{ap\ 208})$, $E(K_w; K_{208}, N_w, L_{ap\ 208}, ID_g)$	KDC responds to the ticket request message with a ticket granting message.

Note: KDC creates a second session key, K_{208}, to allow wireless station 202 to establish a secured session with access point 208. It is important to emphasize that wireless station 202 relies on ID_g and does not need to depend on the identity information of access point 208 to set up the secured session. As a result, wireless station 202 avoids executing the same authentication sequences with access point 208 as it does with access point 206 and shortens the time required to establish the secured session with access point 208.	
Access point 206 → KDC: $E(K_{206}; E(K_g; K_{208}, ID_w, L_{ap\ 208}), E(K_w; K_{208}, N_w, L_{ap\ 208}, ID_g), T_2, E(K_g; N, ID_w, T_2))$ Note: Wireless station 202 may execute the phase 2 protocol at any moment during	Access point 206 selects a time to be T_2, selects a random number N and appends T_2 and $E(K_g; N, ID_w, T_2)$ to the ticket granting message in order to enforce the lifetime of $session\_key_{208}$. This prevents wireless station 202 from specifying an

the time from T_1 to T_1+L_{206}.	unauthorized value for T_2.

<u>Phase 3</u>

Actions	Explanations
Wireless station 202 → access point 208: ID_w, $E(K_w; K_{208}, N_w, L_{208}, ID_g)$, $E(K_{208}; ID_w, T_2)$, $E(K_g; N, ID_w, T_2)$	With the information that access point 208 receives, it can verify the identity of wireless station 202 and determine the validity period of session_key$_{208}$ (i.e. from T_2 to $T_2 + L_{208}$).
Access point 208 → wireless station 202: $E(K_{208}; ID_g)$, $E(K_{208}; N', ID_w)$	The encrypted payload, $E(K_{208}; N', ID_w)$, protects wired network 212 against replay attacks. In other words, because access point 208 keeps generating new N's, wireless station 202 could rely on the varying N's to detect attempts to replay messages from access point 208.
Wireless station 202 → access point 208: $E(K_{208}; N')$	Wireless station 202 proves that it indeed has session_key$_{208}$.

Thus, a method and an apparatus for establishing secured roaming have been disclosed. Although the secured wireless roaming system has been described particularly with reference to the figures, one with ordinary skill in the art may further divide or combine the functionality of its functional blocks. For example, an ordinarily skilled artisan may combine encryption/decryption engine 314 and authentication protocol engine 316 into one integrated component. Finally, despite the detailed discussion on Kerberos protocol, one of ordinary skill in the art could employ other authentication protocols without departing from the spirit and scope of the present invention.